# REPORT DOCUMENTATION PAGE

*Form Approved*
**OMB No. 0704-0188**



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 15-05-2010 | Quarterly technical report | 15 Feb 2010 - 15 May 2010 |

**4. TITLE AND SUBTITLE**
Trust Management for Encounter-Based Routing in Delay Tolerant Networks

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**
N00014-10-1-0156

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
Chen, Ing-Ray (VT)
Bao, Fenye (VT)
Chang, Moonjeong (VT)
Cho, Jin-Hee (ARL)

**5d. PROJECT NUMBER**
10PR02543-01

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
OFFICE OF SPONSORED PROGRAMS
1880 PRATT DRIVE, SUITE 2006
BLACKSBURG, VA 24060-3325

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
Office of Naval Research
875 North Randolph Street
Arlington, VA 22203-1995

**10. SPONSOR/MONITOR'S ACRONYM(S)**
ONR

**11. SPONSORING/MONITORING AGENCY REPORT NUMBER**

**12. DISTRIBUTION AVAILABILITY STATEMENT**
Distribution Statement A: Approved for public release; distribution is unlimited.

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

We propose and analyze a class of trust management protocols for encounter-based routing in delay tolerant networks (DTNs). The underlying idea is to incorporate trust evaluation in the routing protocol, considering not only quality-of-service (QoS) trust properties (connectivity) but also social trust properties (honesty and unselfishness) to evaluate other nodes encountered. Two versions of trust management protocols are considered: an equal-weight QoS and social trust management protocol (called trust-based routing) and a QoS only trust management protocol (called connectivity-based routing). By utilizing a stochastic Petri net model describing a DTN behavior, we analyze the performance characteristics of these two routing protocols in terms of message delivery ratio, latency, and message overhead. We also perform a comparative performance analysis with epidemic routing for a DTN consisting of heterogeneous mobile nodes with vastly different social and networking behaviors. The results indicate that trust-based routing approaches the ideal performance of epidemic routing in delivery ratio, while connectivity-based routing approaches the ideal performance in message delay of epidemic routing, especially as the percentage of selfish and malicious nodes present in the DTN system increases. By properly selecting weights associated with QoS and social trust metrics for trust evaluation, our trust management protocols can approximate the ideal performance obtainable by epidemic routing in delivery ratio and message delay without incurring high message overhead.

# Trust Management for Encounter-Based Routing in Delay Tolerant Networks

Ing-Ray Chen, Fenye Bao, Moonjeong Chang
Department of Computer Science
Virginia Tech
{irchen, baofenye, mjchang}@vt.edu

Jin-Hee Cho
Computational and Information Science Directorate
US Army Research Laboratory
jinhee.cho@us.army.mil

**Abstract**: We propose and analyze a class of trust management protocols for encounter-based routing in delay tolerant networks (DTNs). The underlying idea is to incorporate trust evaluation in the routing protocol, considering not only quality-of-service (QoS) trust properties (connectivity) but also social trust properties (honesty and unselfishness) to evaluate other nodes encountered. Two versions of trust management protocols are considered: an equal-weight QoS and social trust management protocol (called trust-based routing) and a QoS only trust management protocol (called connectivity-based routing). By utilizing a stochastic Petri net model describing a DTN behavior, we analyze the performance characteristics of these two routing protocols in terms of message delivery ratio, latency, and message overhead. We also perform a comparative performance analysis with epidemic routing for a DTN consisting of heterogeneous mobile nodes with vastly different social and networking behaviors. The results indicate that trust-based routing approaches the ideal performance of epidemic routing in delivery ratio, while connectivity-based routing approaches the ideal performance in message delay of epidemic routing, especially as the percentage of selfish and malicious nodes present in the DTN system increases. By properly selecting weights associated with QoS and social trust metrics for trust evaluation, our trust management protocols can approximate the ideal performance obtainable by epidemic routing in delivery ratio and message delay without incurring high message overhead.

**Key words:** delay tolerant networks, opportunistic routing, social trust, QoS trust, social networks, performance analysis, stochastic Petri nets.

## 1. Introduction

A delay tolerant network (DTN) provides interoperable communications through mobile nodes with the characteristics of high end-to-end path latency, frequent disconnection, limited resources (e.g., battery, computational power, bandwidth), and unreliable wireless transmission. Further, for DTNs in mobile ad hoc network (MANET) environments, we also face additional challenges due to a lack of centralized trust entity and this increases security vulnerability [5]. For a sparse MANET DTN, mobility-assisted routing based on *store-carry-and-forward* method has been used. That is, a message carrier forwards a message to an encountered node until the message reaches a destination node. In MANET DTN environments, it is important to select a trustable node as a next message carrier among all encountered nodes to minimize delay for a message to reach a destination node as well as to maximize the message delivery ratio. In this paper, we consider a MANET DTN in the presence of selfish and malicious nodes and propose a family of trust management protocols for encounter-based routing to select a highly trustable next message carrier with the goals of maximizing the message delivery ratio without incurring a high delay or a high message overhead.

In the literature, DTN routing based on encounter patterns has been investigated [2, 10, 11]. However, if the predicted encounter does not happen, then messages would be lost for single-copy routing, or flooded for multi-copy routing. Moreover, these approaches could not guarantee reliable message delivery due to the presence of selfish or malicious nodes. The vulnerability of DTN routing to node selfishness was well studied in [7]. Several recent studies [12, 14, 15] considered using reputation in selecting message carriers among encountered nodes for DTNs. Nevertheless, [12, 14] assumed that a centralized entity exists for credit management, and [15] merely used reputation to judge if the system should switch from reputation-based routing to multipath routing when many selfish nodes exist.

There is very little research to date on the social aspect of trust management for DTN routing. Social relationship and social networking were considered as criteria to select message carriers in a DTN MANET [6, 8]. However, no consideration was given to the presence of malicious or selfish nodes. Very recently [9] considered routing by socially selfish nodes in DTNs, taking into consideration the willingness of a socially selfish node to forward messages to the destination node because of social ties. Unlike prior work cited above, in this paper, we combine the notion of *social trust* and *QoS trust* into a composite trust metric for determining the best node among the new encounters for message forwarding. We consider *honesty* and *unselfishness* for social trust to account for node trustworthiness for

message delivery, and *connectivity* for QoS trust to account for node capability to quickly deliver the message to the destination node. By assigning various weights associated with these QoS and social trust properties, we form a class of DTN routing protocols, from which we examine two versions of the trust management protocol in this paper: an equal-weight QoS and social trust management protocol (called trust-based routing for short) and a QoS trust only management protocol (call connectivity-based routing for short). We analyze and compare the performance characteristics of trust-based routing and connectivity-based routing protocols with epidemic routing [13] for a DTN consisting of heterogeneous mobile nodes with vastly different social and networking behaviors. The results indicate that our trust-based routing protocol approaches the ideal performance of epidemic routing in delivery ratio, while connectivity-based routing approaches the ideal performance of epidemic routing in message delay, as the percentage of selfish and malicious nodes present in the DTN system increases. All DTN routing protocols in the class significantly outperform epidemic routing in message overhead.

## 2. System Model

We consider a MANET DTN environment with no centralized trust authority. Nodes communicate through multi-hops. Every node may have a different level of energy and speed reflecting node heterogeneity. We differentiate selfish nodes from malicious nodes. A selfish node acts for its own interest. So it may drop packets arbitrarily just to save energy but it may decide to forward a packet if it has good social ties with the destination node. A malicious node acts maliciously with the intention to disrupt the main functionality of the DTN, so it can drop packets, jam the wireless channel, and even forge false packets. To deal with malicious nodes, we assume that a distributed intrusion detection system (IDS) exists for detecting malicious nodes. As soon as a malicious node is detected by IDS, the malicious node will be made known to all nodes, which will set the trust value of the malicious node to zero and thus exclude it as a message carrier for message forwarding. Since there is no perfect IDS, we characterize the distributed IDS by its false positive and false negative probabilities for which less than 1% is deemed acceptable. A node initially may be healthy but compromised through capture for example. Once a node is compromised, it is a malicious node. In the paper, we will use the terms malicious node and compromised node interchangeably.

We consider the following node behavior model. The energy level of a node is related with the speed at which the node may be compromised. That is, a node is more likely to be compromised when it has low energy and vice versa since a node with high energy is more capable of defending itself against attackers by performing energy-consuming defense mechanisms. If a node is selfish, the speed of energy consumption is slowed down and vice versa. If a node becomes compromised but not detected by IDS, the speed of energy consumption will increase since the node may have a chance to perform attacks which may consume more energy. We also consider redemption mechanism for a selfish node to have a second chance. That is, a selfish node may become unselfish again socially upon learning status of other neighbor nodes.

A node's trust value is assessed based on direct observations and indirect information like recommendations. The trust of one node toward another node is updated upon encounter events. Our trust metric consists of two trust types: *QoS trust* and *social trust*. *QoS trust* is evaluated through the communication and information networks by the capability of a node to deliver messages to the destination node. We consider ***connectivity*** to measure the QoS trust level of a node. Social trust is based on social relationships. We consider ***unselfishness*** (or cooperation) and ***honesty*** (or healthiness) to measure the social trust level of a node. Different from most existing encounter-based routing protocols which considered only connectivity, we consider social trust in additional to QoS trust in order to select more faithful message carriers among encountered nodes. We define a node's trust level as a real number in the range of [0, 1], with 1 indicating complete trust, 0.5 ignorance, and 0 complete distrust.

## 3. Trust Management for Message Routing

The trust value of node $j$ as evaluated by node $i$ at time $t$, denoted as $T_{ij}(t)$, is computed by a weighted average of connectivity, honesty, and unselfishness trust components. Specifically node $i$ will compute $T_{ij}(t)$ by:

$$\begin{aligned} T_{ij}(t) = {} & w_1 T_{i,j}^{e-connectivity}(t) \\ & + w_2 T_{i,j}^{d-connectivity}(t) \\ & + w_3 T_{i,j}^{honesty}(t) \\ & + w_4 T_{i,j}^{unselfis\ hness}(t) \end{aligned} \quad (1)$$

where $w_1 : w_2 : w_3 : w_4$ is the weight ratio with $w_1 + w_2 + w_3 + w_4 = 1$. Of these trust components (or properties) in Equation 1, $T_{i,j}^{e-connectivity}(t)$ is about node $i$'s belief in node $i$'s encounter connectivity to node $j$, representing the delay of node $i$ passing the message to node $j$, $T_{i,j}^{d-connectivity}(t)$ is about node $i$'s belief in node $j$'s connectivity to the destination node $d$, representing the delay of node $j$ passing the message to node $d$, $T_{i,j}^{honesty}(t)$ is about node $i$'s belief in node $j$'s honesty, and $T_{i,j}^{unselfis\ hness}(t)$is about node $i$'s belief in node $j$'s cooperation. In message forwarding in DTNs, two most important performance metrics are message delivery

ratio and delay. The rationale of using these four trust metrics is to rank nodes such that high $T_{i,j}^{e-connectivity}(t)$ and $T_{i,j}^{d-connectivity}(t)$ represent low delay, while high $T_{i,j}^{honesty}(t)$ and $T_{i,j}^{unselfishness}(t)$ represent high delivery ratio. We set $T_{i,j}^{e-connectivity}(0)$, $T_{i,j}^{d-connectivity}(0)$, $T_{i,j}^{honesty}(0)$ and $T_{i,j}^{unselfishness}(0)$ to ignorance since initially there is no information exchanged among nodes. When node $i$ encounters another node, say node $m$, it exchanges its encounter history with node $m$ and uses node $m$ as a recommender to update its beliefs toward node $j$ as follows:

$$T_{i,j}^{X}(t) = \beta_1 T_{i,j}^{direct,X}(t) + \beta_2 T_{i,j}^{indirect,X}(t) \quad (2)$$

where $X$ refers to a trust property (e-connectivity, d-connectivity, honesty, or unselfishness) with:

$$T_{i,j}^{direct,X}(t) = \begin{cases} T_{i,m}^{encounter,X}(t), if\ m = j \\ T_{i,j}^{X}(t - \Delta t), if\ m \neq j \end{cases} \quad (3)$$

$$T_{i,j}^{indirect,X}(t) = \begin{cases} T_{i,m}^{X}(t - \Delta t), if\ m = j \\ T_{i,m}^{X}(t) \times T_{m,j}^{X}(t), if\ m \neq j \end{cases} \quad (4)$$

In Equation 2, $\beta_1$ is a weight parameter to weigh node $i$'s own trust assessment toward node $j$ at time $t$, i.e., "self-information," and $\beta_2$ is a weight parameter to weigh indirect information from the recommender, i.e., "other-information," with $\beta_1 + \beta_2 = 1$. In Equation 3, if the new encounter (node $m$) is node $j$ itself, node $i$ can directly observe trust properties of node $j$. We use $T_{i,m}^{encounter,X}(t)$ to denote the assessment result of node $i$ toward node $m$ in trust property $X$ based on direct observations. Later in Section 4, we will describe how this can be obtained using node $i$'s knowledge toward a newly encountered node. If the new encounter $m$ is not node $j$, we use node $i$'s belief in node $j$ as evaluated at time $t$-$\Delta t$, corresponding to the belief of node $i$ toward node $j$ based on past interaction experiences prior to time $t$, as the basis of direct observations for node $i$ to further evaluate node $j$ at time $t$. Here $\Delta t$ refers to the duration between two encounter times. In Equation 4, if the new encounter $m$ is node $j$ itself, then there is no indirect recommendation information, so node $i$ will just use its trust information obtained at time $t$-$\Delta t$. If the new encounter $m$is not node $j$, then node $m$ will provide its recommendation to node $i$ for evaluating node $j$, and we must take node $i$'s belief in node $m$ into consideration in the calculation of Equation 4. This models the decay of trust as trust is derived from a distant node as indirect information.

$T_{ij}(t)$ in Equation 1 can be used by node $i$ (if it is a message carrier) to decide, upon encountering node $m$, if it should forward the message to node $m$ with the intent to shorten the message delay and improve the message delivery ratio. We consider a $\Omega$–permissible policy in this paper, i.e., node $i$ will pass the message to node $m$ if $T_{i,m}(t)$ is in the top $\Omega$ percentile among all $T_{i,j}(t)$'s. We experiment with various values of $\Omega$ to trade message delivery ratio with message latency.

## 4. Performance Model

We analyze the performance of the proposed trust-based routing protocol for DTN message forwarding by a probability model based on stochastic Petri net (SPN) techniques [4] due to its ability to handle a large number of states. The SPN model is shown in Figure 1. The SPN model describes a node's lifetime in the presence of selfish and malicious nodes, and IDS to detect malicious nodes. It is used to obtain each node's information (e.g., connectivity, honesty, and unselfishness) and to derive the trust relationship with other nodes in the system. Without loss of generality, we consider a square-shaped operational area consisting of $m \times m$ sub-grid areas with the width and height equal to wireless radio range ($R$). Initially nodes are randomly distributed over the operational area based on uniform distribution. A node randomly moves to one of four locations in four directions (i.e., north, west, south, and east) in accordance with its mobility rate. To avoid end-effects, movement is wrapped around (i.e., a torus is assumed). The SPN model produces the probability that node $i$ is at a particular location $L$ at time $t$. This information along with the location information of other nodes at time $t$ provides us the probability of two nodes encountering with each other, and how often two nodes exchange encounter histories to update $T_{i,j}^{X}(t)$.

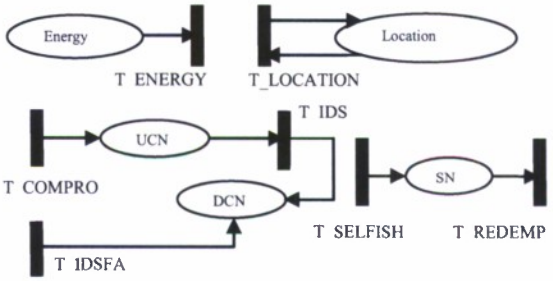


**Figure 1: SPN Model.**

Below we explain how we construct the node SPN subnet for describing a node's behavior in terms of its location, energy level, degree of honesty (e.g., whether or not a node is compromised or/and detected by IDS), and degree of selfishness.

**Location**: Transition T_LOCATION is triggered when the node moves to a randomly selected area out of four different directions from its current location with the rate calculated as $\sigma(t)/R$ based on its speed $\sigma(t)$ at time $t$ and wireless radio range ($R$). The speed at time $t$ is linearly proportional to its remaining energy, calculated as $\sigma_0 \times E_{remain}/E_0$ where $\sigma_0$ is the initial speed, $E_0$ is the initial energy and $E_{remain}$ is the remaining energy given by *mark(Energy)*.

**Connectivity**: Connectivity of node $j$ to the destination node $d$ is measured by the time-averaged probability that node $j$ and node $d$ are within one-hop during $[t\text{-}n\Delta t,\ t]$, modeling not only chances, but also recency of encountering events between node $j$ and node $d$. This can be obtained by knowledge of location probabilities of node $j$ and node $d$ during $[t\text{-}n\Delta t,\ t]$.

**Energy**: Place *Energy* represents the current energy level of a node. An initial energy level of each node is assigned according to node heterogeneity information. A token is taken out when transition T_ENERGY fires. The transition rate of T_ENERGY is adjusted on the fly based on a node's state. It is lower when a node is selfish to save energy; it is higher when the node becomes compromised so that it performs attacks more and consumes energy more. We use the energy model in [3] to adjust the rate to consume one token in place *Energy* based on a node's state.

**Honesty**: A node is compromised when transition T_COMPRO fires. The transition rate to transition T_COMPRO is modeled as $1/T_{comp}$ with the interval $T_{comp} = \alpha_1 (mark(Energy) + 1)^{\varepsilon}/\lambda_{com}$ where $\lambda_{com}$ is the node compromise rate initially given, and $mark(Energy)$ indicates the level of current energy. In practice $\lambda_{com}$ can be derived from the first-order approximation of the attack history collected by IDS. The two parameters $\alpha_1$ and $\varepsilon$ are used to model the behavior of node compromise such that if the node has low energy, it is more likely to become compromised, and vice versa. If the node is compromised, a token goes to *UCN*, meaning that the node is being compromised but not yet detected by IDS. While the node is not detected by IDS, it has a chance to perform attacks. If a compromised node is being detected by IDS, a token is taken out from *UCN* into *DCN* and the node is evicted immediately. We model a DTN equipped with IDS characterized by false alarm probabilities. A false negative probability ($P_{fn}^{IDS}$) of IDS is considered in T_IDS which has the rate of $(1 - P_{fn}^{IDS})/T_{IDS}$ and a false positive probability ($P_{fp}^{IDS}$) of IDS is considered in T_IDSFA which has the rate of $P_{fp}^{IDS}/T_{IDS}$.

**Selfishness**: Place *SN* represents whether a node is selfish or not. If a node becomes selfish, a token goes to *SN* by triggering T_SELFISH. A node's selfish behavior is a function of its remaining energy. Specifically, the transition rate to T_SELFISH is given by:

$$rate(T\_SELFISH) = \frac{f(E_{remain})}{\Delta t} \tag{5}$$

where $\Delta t$ is the duration between two encountering events over which a node may decide to become selfish. The form $f(y) = \alpha_2 y^{-\varepsilon}$ follows the demand-pricing relationship in Economics [1] to model the effect of its argument $y$ on the selfishness behavior, such that $f(E_{remain})$ models the behavior that a node with a higher level of energy is less likely to be selfish. Similarly a selfish node may become unselfish again through transition T_REDEMP. The redemption rate is modeled in a similar way as:

$$rate(T\_REDEMP) = \frac{g(E_{consumed})}{\Delta t} \tag{6}$$

where $g(y) = \alpha_3 y^{-\varepsilon}$ and $E_{consumed}$ is the amount of energy consumed as given by $E_0 - E_{remain}$ and $\Delta t$ is the encountering interval over which a selfish node may decide to become unselfish again. $g(E_{consumed})$ models the behavior that a node with a lower level of energy will more likely stay selfish to further save its energy considering its own individual benefit.

With the node behaviors modeled by the SPN model described above we can calculate $T_{i,j}^{X}(t)$ as follows. When node $i$ encounters node $m$, node $i$ will perform direct trust assessment toward node $m$ in trust property $X$ to yield $T_{i,m}^{encounter\ ,X}(t)$. Because node $i$ and node $m$ are within 1-hop upon encounter, node $i$ has exact knowledge about whether node $m$ is selfish or not through status exchange, snooping and overhearing. Hence node $i$'s direct assessment in node $m$'s selfishness at the encounter time $t$ is exactly the same as the selfishness status node $m$ at time $t$. Consequently, $T_{i,m}^{encounter\ ,\ unselfishness}(t)$ in Equation 3 is simply equal to the probability that place *SN* does not contain a token at time $t$, which we can compute easily from the SPN output. Similarly, $T_{i,m}^{encounter\ ,\ e-connectivity}(t)$ can be computed by the time-averaged probability that node $i$ and node $m$ are within one-hop during$[t - n\Delta t, t]$, and $T_{i,m}^{encounter\ ,\ d-connectivity}(t)$ by the time-averaged probability that node $m$ and node $d$ are within one-hop during $[t\text{-}n\Delta t,\ t]$, utilizing the SPN output regarding the node location probability at time $t$. For the honesty trust component, node $i$ knows node $m$ is malicious only when IDS detects it and announces a message to the system, i.e., when node $m$'s place *DCN* (in Figure 1) is not zero. Thus, we can compute $T_{i,m}^{encounter\ ,\ honesty}(t)$ by the probability that place *DCN* in node $m$ contains a token at time $t$. Once $T_{i,m}^{encounter\ ,X}(t)$ is obtained at each encounter time, node $i$ can update its $T_{i,j}^{X}(t)$ based on Equation 2, and subsequently, can obtain $T_{ij}(t)$ based on Equation 1.

## 5. Results

**Table 1: Default parameter values used.**

| Param | Value | Param | Value | Param | Value |
|---|---|---|---|---|---|
| $m \times m$ | 8×8 | $R$ | 250$m$ | $T_{IDS}$ | 600$s$ |
| $\alpha_1$ | 0.005 | $\alpha_2$ | 4 | $\alpha_3$ | 0.5 |
| $\varepsilon$ | 1.6 | $\Omega$ | 90% | $\Delta t$ | 300 $s$ |
| $\beta_1$:$\beta_2$ | 0.8:0.2 | $n$ | 2 | $T_{IDS}$ | 600 $s$ |
| $\sigma_0$ | (0, 2] $m/s$ | $P_{fn}^{IDS}, P_{fp}^{IDS}$ | 0.5% | $E_0$ | [12,24] $hrs$ |
| | | $1/\lambda_{com}$ | [160, 320, 480] $min$. | | |

Below we show numerical results and provide physical interpretation of the results obtained. Table 1 lists the default parameter values used. For trust-based routing, we set $w_1:w_2:w_3:w_4 = 0.25:0.25:0.25:0.25$ for e-connectivity: d-connectivity: honesty: unselfishness, while for connectivity-based routing, we set $w_1:w_2:w_3:w_4 = 0.5:0.5:0:0$. We setup 20 nodes with vastly different initial energy levels in the system moving randomly in a 8×8 operational region with the mobility in the range of (0, 2] *m/s* and with each area covering 250 *m* radio radius. Good nodes are the ones with the compromise rate being 0 and the selfish rate being zero. Selfish nodes are the ones with the selfish rate defined based on Equation 5 and redemption rate defined by Equation 6. Bad nodes have a non-zero compromise rate $\lambda_{com}$ in the range of [1/480min., 1/160min.], allowing bad nodes to transit from healthy nodes to malicious nodes. We use all encounters as the recommenders. The initial trust level is set to ignorance (i.e., 0.5) for all trust properties.

To reveal which trust component might have a more dominant effect, we show $T_{i,j}^{e-connectivity}(t)$, $T_{i,j}^{d-connectivity}(t)$, $T_{i,j}^{honesty}(t)$ and $T_{i,j}^{unselfishness}(t)$ for node $i$ evaluating node $j$ randomly picked. Other nodes exhibit similar trends and thus only one set of results is shown. Figure 2 shows these trust component values as a function of time $t$ with the compromise rate of node $j$ ranging from once per 480 min. to once per 160 min. We see that connectivity dominates other trust properties when node $j$'s compromise rate is small. However, as the compromise rate increases, honesty dominates other trust properties as the percentage of malicious nodes increases. This demonstrates that our trust-based routing protocol for encounter-based message forwarding reflects dynamic environmental changes.

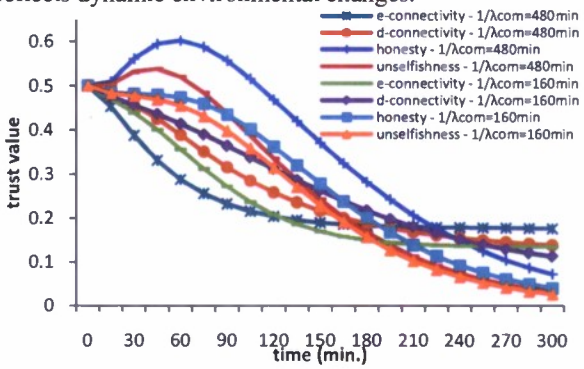


**Figure 2: Comparing $T_{i,j}^{X}(t)$ as a function of time with respect to node $j$'s compromise rate.**

Next we consider a message forwarding scenario in which in each run we randomly pick a source node *s* and a destination node *d*. The source and destination nodes picked are always good nodes. There is only a single copy of the message initially given to node *s*. We let the system run for 30 min. to warm up the system and start the message forwarding afterward in each run. During a message passing run, every node $i$ updates its $T_{i,j}(t)$ for all $j$ based on Equation 1. In particular the current message carrier uses $T_{i,j}(t)$ to judge if it should pass the message to a node it encounters at time $t$. If the message carrier is malicious, the message is dropped (a weak attack). If the message carrier is selfish, the message delivery continues with 50% of the chance. A message delivery run is completed when the message is delivered to the destination node, or the message is lost before it reaches the destination node. Statistics are collected for 1500 runs from which the message delivery ratio, delay and overhead performance measurements are calculated.

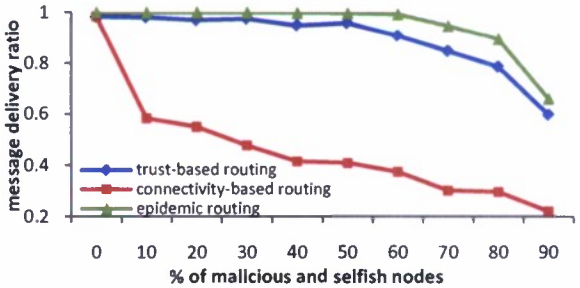


**Figure 3: Message delivery ratio: comparing trust-based vs. connectivity-based and epidemic protocols.**

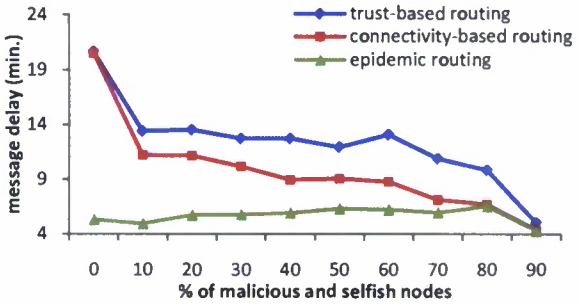


**Figure 4: Message delay: comparing trust-based vs. connectivity-based and epidemic routing protocols.**

Figure 3 shows the message delivery ratio as a function of the percentage of compromised and selfish nodes in the DTN for trust-based and connectivity-based routing protocols. For performance comparison, we also show the delivery ratio obtained from epidemic routing. Here we see that trust-based routing outperforms connectivity-based routing in delivery ratio and its performance approaches the maximum achievable performance obtainable from epidemic routing. This is attributed to the ability of trust-based protocols being able to differentiate healthy nodes from selfish or malicious nodes and select healthy nodes to relay the message. The result demonstrates the effectiveness of incorporating social trust into the decision making process for DTN message routing.

Figure 4 shows the average delay experienced per message considering only those messages delivered successfully. Here we first note that connectivity-based routing will always perform better than trust-based routing because connectivity-based protocols use the delay to encounter the next message carrier (e-connectivity) and the delay for the next message carrier to encounter the destination node (d-connectivity) as the criteria to select the next message carrier. The result suggests that if delay is of primary concern, we should set the weights associated with e-connectivity and d-connectivity (QoS trust metrics) higher than those for honesty and unselfishness (social trust metrics), as what connectivity-based routing does (by setting $w_1: w_2: w_3: w_4 = 0.5: 0.5: 0: 0$). This will have the effect of trading high delivery ratio off for low delay. Figure 4 also shows that connectivity-based routing achieves the ideal performance obtainable from epidemic routing as the percentage of malicious and selfish nodes increases.

Figure 5 compares the three protocols in message overhead measured by the number of copies forwarded to reach the destination node for those messages successfully delivered. We see trust-based protocols perform comparably with connectivity-based protocols and both protocols considerably outperform epidemic routing in message overhead.

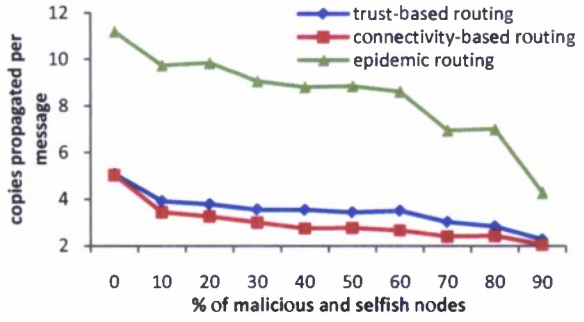


**Figure 5: Number of copies propagated per message.**

## 6. Conclusion

In this paper, we have proposed and analyzed a class of trust management protocols for encounter-based routing in DTNs. The most salient feature of our protocol is that we consider not only connectivity (QoS trust) but also honesty and unselfishness (social trust) properties into a composite trust metric for decision making in DTN routing dynamically. Our performance analysis results demonstrate that by properly selecting weights associated with QoS and social trust metrics for trust evaluation, our trust management protocols can achieve the ideal performance level in delivery ratio and delay obtainable by epidemic routing, especially as the percentage of malicious and selfish nodes increases.

In the future, we plan to investigate other forms of message passing such as multi-copy message forwarding and other forms of attacks by malicious nodes such as jamming, forgery, self-promoting and slandering attacks. We also plan to consider other trust metrics such as technical competence, betweenness, similarity, and social tie strengths [6]. Another direction is to investigate the best ratio of $w_1: w_2: w_3: w_4$ or $\beta_1: \beta_2$ based on knowledge about the application or network context.

## References


[1] M. Aldebert, M. Ivaldi, and C. Roucolle, "Telecommunications Demand and Pricing Structure: an Economic Analysis," *Telecommunication Systems*, vol. 25, no. 1-2, Jan. 2004, pp. 89-115.

[2] J. Burgess, B. Gallagher, D. Jensen, and B.N. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networking," *IEEE Infocom*, Barcelona, Spain, Apr. 2006, pp. 1-11.

[3] J.H. Cho, A. Swami and I.R. Chen, "Modeling and Analysis of Trust Management for Cognitive Mission-driven Group Communication Systems in Mobile Ad Hoc Networks," *7th IEEE/IFIP Int. Symp. Trusted Computing and Communications*, Vancouver, Canada, Aug. 2009.

[4] G. Ciardo, R.M. Fricks, J.K. Muppala and K.S. Trivedi, *Stochastic Petri Net Package Users Manual*, Department of Electrical Engineering, Duke University, 1999.

[5] E.M. Daly and M. Haahr, "The Challenges of Disconnected Delay Tolerant MANETs," *Ad Hoc Networks*, vol. 8, no. 2, March 2010, pp. 241-250.

[6] E.M. Daly and M. Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs," *IEEE Transactions on Mobile Computing*, vol. 8, no. 5, May 2009, pp. 606-621.

[7] M. Karaliopoulos, "Assessing the Vulnerability of DTN Data Relaying Schemes to Node Selfishness," *IEEE Comm. Letters*, vol. 13, no. 12, 2009, pp. 923-925.

[8] E. Bulut, Z. Wang and B.K. Szymanski, "Impact of Social Networks on Delay Tolerant Routing," *IEEE Globecom 2009*, Hawaii, USA, Nov. 2009.

[9] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," *IEEE Infocom*, San Diego, CA, March 2010.

[10] S. Jain, K. Fall, and R. Patra, "Routing in a Delay Tolerant Network," *ACM Computer Communication Review*, vol. 34, no. 4, Oct. 2004. pp. 145-158.

[11] S.C. Nelson, M. Bakht and R. Kravets, "Encounter-based Routing in DTNs," *IEEE Infocom*, Rio De Janeiro, Brazil, Apr. 2009, pp.846-854.

[12] U. Shevade, H. Song, L. Qiu, and Y. Zhang, "Incentive-Aware Routing in DTNs," *16th IEEE Int'l Conf. on Network Protocols*, Orlando, FL, USA, Oct. 2008.

[13] A. Vahdat and D. Becker, "Epidemic Routing for Partially Connected Ad Hoc Networks," Technical Report, Computer Science Department, Duke University, 2000.

[14] Z. Xu, et al. "SReD: A Secure Reputation-Based Dynamic Window Scheme for Disruption-Tolerant Networks," *IEEE Military Communications Conf.*, Oct. 2009, pp. 1-7.

[15] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks", *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, Oct. 2009, pp. 4628-4638.

INSTRUCTIONS FOR COMPLETING SF 298

| 15. SUBJECT TERMS<br>Trust, trust management, delay tolerant networks, opportunistic routing, social trust, QoS trust, social networks, performance analysis, stochastic Petri nets. | | | | | |
|---|---|---|---|---|---|
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT<br>SAR | 18. NUMBER OF PAGES<br>6 | 19a. NAME OF RESPONSIBLE PERSON<br>Chen, Ing-Ray |
| a. REPORT<br>U | b. ABSTRACT<br>U | c. THIS PAGE<br>U | | | 19b. TELEPONE NUMBER (*Include area code*)<br>(703) 538-8376 |